UNITED STATES PATENT APPLICATION

FOR

SYSTEM AND METHOD FOR MOBILE TRANSACTIONS USING THE BEARER INDEPENDENT PROTOCOL

IN THE NAMES OF

SCOTT GOLDTHWAITE

ANDREW PETROV

ANDREI DOUDKINE

WAY SYSTEMS, INC.

ATTORNEY DOCKET NO.: WS-105

Please direct communication to

Aliki K. Collins, Ph.D.

AKC Patents

215 Grove St.

Newton, MA 02466

617-558-5389

EXPRESS MAIL NO.: ER 224855061 US

SYSTEM AND METHOD FOR MOBILE TRANSACTIONS USING THE BEARER INDEPENDENT PROTOCOL

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/455,761 filed on March 19, 2003 and entitled SYSTEM AND METHOD FOR MOBILE TRANSACTIONS USING THE BEARER INDEPENDENT PROTOCOL which is commonly assigned and the contents of which are expressly incorporated herein by reference.

This application is also a continuation in part of U.S. applications Serial No. 10/205,768, 10/625,823, 10/695,585, and 10/729043 filed on July 26, 2002, July 23, 2003, October 28, 2003, and December 5, 2003 and entitled "SYSTEM AND METHOD FOR PAYMENT TRANSACTION AUTHENTICATION", "MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER", "MOBILE COMMUNICATION DEVICE EQUIPPED WITH A MAGNETIC STRIPE READER", and 'SYSTEM AND METHOD FOR MOBILE PAYMENT AND FULFILLMENT OF DIGITAL GOODS" respectively, the contents of which applications are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a system and a method for performing transactions between a mobile device and a remote server utilizing the Bearer Independent Protocol commands.

Background of the Invention

Mobile phones, originally designed for voice communication, are now extensively utilized for data transmission. The Short Message Service (SMS) protocol is the most widely used form of sending text messages between mobile phone users. SMS is also utilized for data communication between a server and a mobile phone. For example, in a

simple "server-to-mobile" system, a server sends a mobile phone user an SMS message to notify him that he has voice mail or to send him information updates, i.e., news, weather and sports updates. More complex SMS applications enable the mobile phone user to send an SMS message to a designated server to request a stock quote, perform an inventory lookup or process a credit card transaction. SMS is a "store and forward" messaging protocol that ensures that a message reaches its intended destination. While this protocol is appropriate for sending text messages between two mobile phone users, it is not well suited for sending data and performing financial transactions between a mobile device and a host system for the following reasons.

- The European Telecommunications Standards Institute (ETSI) SMS specification (3GPP TS 23.040) defines the technical size limitation of an SMS message as 140 bytes. As a result, if the data transmission requires a larger size message, an application on the mobile device and the server must split up the message into smaller sizes and reassemble messages in the proper order.
- SMS messages have no context of a session, i.e., each SMS message is a distinct event. As a result, if a transaction requires multiple steps and therefore multiple SMS messages are needed to complete the transaction, the mobile device and server application must keep track of the transaction as it progresses through the various steps required to complete the transaction.
- Although SMS data can be encrypted "over the air" within a mobile operator's network, there is no specification for SMS data encryption once the message is transmitted beyond the mobile operator's network. For example, if the destination of the SMS message is a server inside a banking or enterprise network which is outside the mobile operator's network, the data will be unencrypted and vulnerable to interception by other unauthorized parties. As a result, the mobile device and server application must implement their own encryption method to ensure that the data in the SMS message are encrypted between the two endpoints.
- The "store and forward" nature of SMS provides reliability in getting a message transmitted. However, this also results in time delays between sender and recipient. This message latency is unpredictable and not suitable for conducting transactions where timing is important. For example, in financial transactions

where customers and merchants expect instantaneous data transmission for payment authorization transactions, SMS message transmission that can average between 5 seconds to 60 seconds is not acceptable.

The implementation of packet-switch networks such as General Packet Radio Service (GPRS), DataTac, Mobitex provides an "always on" connection for data transmission that solves many of the problems associated with SMS data transmissions for transaction processing. GPRS also provides a direct gateway to the Internet, thereby enabling a mobile transaction system to directly interface between a mobile device and a server without utilizing SMS. Mobile devices can utilize GPRS networks in several ways:

- The mobile device can be directly connected to a computer using a serial cable, infrared or Bluetooth connection. When connected to the computer, the mobile device acts like a typical modem and an application on the computer can utilize Asynchronous Transfer Mode (ATM) commands to control the mobile device's connection to the GPRS network and establish a connection to the Internet. Once connected to the Internet, the computer can act as either a host/server or a client to create a mobile transaction processing system.
- The mobile device can also directly utilize a GPRS connection using a built-in or web/WAP browser to connect to a server application. Alternatively, the mobile device may enable developers to develop and deploy an application directly on the mobile device's operating system.
- On mobile devices that utilize a Subscriber Identification Card (SIM) card, applications on the SIM card can access control the GPRS connection utilizing SIM Toolkit (STK) commands as defined in the ETSI specification, ETSI TS 101 267 (3GPP TS 11.14). Using this connection, a web/WAP browser or an application on the SIM card can access data on a server and perform secure transaction processing.

Each of these methods enables a mobile financial transaction processing system depending on the type of application. The SIM card method is a more flexible solution because the SIM card can be placed into any mobile device that meets the 3GPP TS 11.14 (class e) specifications and the application will work the same way on any of these devices, whereas the other methods require custom programming for each type of mobile

device. Although the SIM card approach provides greater flexibility, this approach is also more complex to develop because the SIM card is issued by the mobile network operator and only the mobile network operator can allow applications to be developed and deployed on the SIM card. As a result third party developers are not able to deploy applications without cooperating with the mobile network operator. Accordingly, there is a need for a system that allows third party developers to develop and deploy applications on the SIM card without the need for approval from the mobile network operator. Furthermore, the system needs to be able to transmit and receive data utilizing a standard communication protocol that will work the same way on any mobile device without the need for customization.

Summary of the Invention

In general, one aspect of the invention provides a system for performing mobile transactions that includes a mobile communication device connected to a server device via a first network. The mobile communication device includes a subscriber identification module (SIM) card slot and a virtual subscriber identification (VSIM) interface connected to the SIM card slot and it provides subscriber identity authentication to the server device via the VSIM interface. The mobile communication device further includes a mobile transaction client application for managing communications between the mobile communication device and the server device. The mobile transaction client application manages the communication between the mobile device and the server device by utilizing SIM Application Toolkit (STK) commands to invoke the Bearer Independent Protocol described in the European Telecommunications Standards Institute document ETSI TS 101 267 (3GPP TS 11.14).

Implementations of this aspect of the invention include the following. The server device may further include a mobile transaction server application for managing the communication between the server and the mobile communication device. The VSIM interface may be located within the mobile communication device or within an attachment device. The attachment device may be connected to the mobile

communication device via the SIM card slot and may further include one or more additional SIM slots, at least a second SIM card connected to one of the one or more additional SIM slots and a card reader. The card reader may be a smart card reader, a magnetic stripe card reader or a contactless smart card reader. The mobile communications device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control or combinations thereof. The first network may be a wireless telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a wireless private network, or a wireless personal area network (PAN). The wireless telecommunications network may be a Global System for Mobile Communications (GSM), a Code Division Multiple Access (CDMA), CDMA 2000, wideband CDMA (WCDMA), Time Division Multiple Access (TDMA), General Packet Radio Service (GPRS), Third Generation (3G), Enhanced Data GSM Environment (EDGE), Mobitex or DataTac. The first network may also be infrared, serial line or Bluetooth. The first network may connect to a second network through a mobile operator gate and the server may connect to the second network thereby connecting to the first network and the mobile communication device. The second network may be the Internet, a wireless network, a wired network, a telecommunications network, a local area network (LAN), a WWAN, WLAN, or a personal area network (PAN). The communication may have a format such as Short Message Service (SMS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UPD), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or a proprietary message format. The server device may be further connected to other server devices via the second network. The mobile transactions may be financial transactions, information exchange or digital goods exchange. The server device may be a server computer, a personal computer, a second mobile communication device, a printer, or another communication device. The mobile communication device may further include a memory, a Central Processing Unit (CPU) and a first SIM card connected to the SIM card slot where the first SIM card authenticates the mobile communication device to the first network. The mobile communications device may further include other interfaces connected to the CPU. These other interfaces may be smart card interfaces, infrared

transceiver interfaces, serial communication interfaces, or magnetic stripe reader interfaces. The mobile transaction client application may be stored in the VSIM interface, the CPU, the second SIM card, an external SIM card, a contactless smart card, a magnetic stripe card, or an external card.

In general in another aspect the invention provides a method for performing mobile transactions including the following steps. First providing a mobile communication device having a subscriber identification module (SIM) card slot and a virtual subscriber identification (VSIM) interface connected to the SIM card slot. Next, providing a server device and connecting the mobile communication device to the server device via a first network. Next, providing subscriber identity authentication of the mobile communication device to the server device via the VSIM interface and communicating between the mobile communication device and the server device for performing mobile transactions. The mobile communication device further includes a mobile transaction client application for managing the communication between the mobile communication device and the server device. The mobile transaction client application manages the communication between the mobile device and the server device by utilizing SIM Application Toolkit (STK) commands to invoke the Bearer Independent Protocol described in the European Telecommunications Standards Institute document ETSI TS 101 267 (3GPP TS 11.14).

Among the advantages of this invention may be one or more of the following. This invention provides an alternative and convenient way to develop and deploy mobile transaction processing systems. The advantage of using a mobile device attachment to interface with the mobile device at the SIM slot is application portability. The SIM Toolkit (STK) interface supported by the mobile device is a standard that is implemented identically on any mobile device that supports the standard. Therefore, any mobile transaction system that utilizes the STK specification will work on any mobile device that supports the standard regardless of the mobile device's hardware, software or firmware. Additionally, the approach of utilizing a VSIM interface enables the mobile device to access customized applications when the mobile device may otherwise be unable to be programmed with custom applications.

Brief Description of the Drawings

FIG. 1 is schematic diagram of a mobile transaction system according to this invention;

FIG. 2 is a block diagram of the system architecture the mobile transaction system of FIG. 1;

FIG. 3 is another embodiment of the mobile transaction system according to this invention;

FIG. 4A is the ETSI specification for the Bearer Independent Protocol supported proactive commands;

FIG. 4B is the ETSI specification for the Bearer Independent Protocol supported bearers;

FIG. 4C is the ETSI specification for theBearer Independent Protocol supported transport interfaces; and

FIG. 5 illustrates a circuitry for a mobile device attachment that adds multiple smart cards to a mobile device via a connection to the SIM slot on the mobile device.

Detailed Description of the Invention

The present invention describes a system and method for processing mobile transactions. The system includes one or more mobile devices exchanging data with one or more remote servers or devices. The system utilizes a SIM Application Toolkit (STK) commands in order to establish a communication link between the one or more mobile devices and the one or more remote servers or devices.

Referring to FIG 1 and FIG 2, a mobile transaction system 100 includes a mobile device 110, a mobile device attachment 120, a server 140 and additional servers 150. The mobile device 110 accesses the server 140 via a network connection 115 that includes a first network 90, a mobile operator gateway 130, and a second network 80. The mobile device 110 includes a Subscriber Identification Module (SIM) card 99 and a SIM slot 111. The mobile device attachment 120 connects to the mobile device 110 by attaching to the mobile device SIM slot 111.

Referring to FIG. 2, the mobile device attachment 120 includes a Virtual Subscriber Identification Module (VSIM) interface 121, a primary SIM slot 122, a secondary SIM slot 123, a card reader 124 and a SIM 126 placed in the primary SIM slot 122. The VSIM 121 includes a mobile transaction client application 125 that manages the interaction between the mobile device 110, the SIM 126 and a plurality of Smart Cards attached to SIM slots 122, 123 or to the card reader 124. The mobile transaction client application 125 utilizes the Bearer Independent Protocol (BIP) to open a communication channel to the mobile device 110 and to transmit and receive data to server 140. In this embodiment the mobile transaction client application 125 resides within VSIM 121. In other embodiments the mobile transaction client application 125 may reside within any of the smart cards attached to slots 122, 123 or within an external smart card that can be accessed via the card reader 124. Server 140 includes a mobile transaction server application 141 that transmits and receives data to and from the mobile transaction client application 125, respectively, using the communication channel established by the mobile transaction client application 125. The data that are transmitted between the mobile transaction client application 125 and mobile transaction server application 141 may be encrypted. In one example, the card reader 124 is a full-size ISO 78.16 smart card reader. In other examples, the card reader 124 is a contactless card reader or a magnetic stripe card reader, as described in the co-pending patent applications entitled "Mobile Device Equipped with a Contactless Smart Card Reader", and "Mobile Communication Device Equipped with a Magnetic Stripe Reader", respectively, the entire contents of which are incorporated herein by reference.

The SIM card 99 is issued by the mobile network operator and usually only the mobile network operator controls the development and deployment of applications on the SIM card 99. Third party application developers need to cooperate with the mobile network operator in order to develop and deploy applications on the SIM card 99. To alleviate the problem of developing SIM applications without obtaining cooperation from the mobile network operator or SIM card issuer, the invention described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", the entire content of which is incorporated herein by reference, describes an attachment that connects to a mobile device SIM slot and provides an interface to the mobile device. Referring to FIG. 5, a schematic block diagram of the mobile device circuitry 200 includes a central processing unit (CPU) 202, which is connected through a phone interface logic arrangement 206 to a phone Subscriber Identification Module (SIM) socket 204. The CPU 202 has a clock arrangement 212 and power controller logic 210, which connects, to a phone battery interface 208. The CPU 202 has a memory 216, memory control logic 214, and a real time clock 218. The CPU 202 is also connected to an original subscriber identification module (OSIM) interface 220, and an external subscriber identification module (ESIM) interface 222. The OSIM interface 220 includes a first OSIM1 connector 224 and a second OSIM2 connector 226. OSIM1 connector 220 connects to a SIM 1 card 152 and OSIM 2 connector connects to SIM 2 card 156. The ESIM interface 222 includes an ESIM connector 228 that connects to an external card reader 153. In addition to the external card reader, "contactless" smart card reader and/or a magnetic stripe card reader can connect to the CPU 202, as described in the co-pending patent applications entitled "Mobile Device Equipped with a Contactless Smart Card Reader", and "Mobile Communication Device Equipped with a Magnetic Stripe Reader", respectively, the entire contents of which are incorporated herein by reference. The memory 216 and memory control logic 214 function so as to provide a Virtual SIM (VSIM) interface that allows data communication between the phone and the SIM card within the VSIM interface and manages the communication between the phone and applications within the VSIM interface and/or applications stored in any of the other cards that are in connection with the VSIM interface.

As was mentioned above, the mobile transaction client application 125 utilizes the Bearer Independent Protocol (BIP) to open a communication channel to the mobile device 110 and to transmit and receive data to server 140. The BIP is a signaling protocol specified by the European Telecommunications Standards Institute (ETSI) in a document entitled "ETSI TS 101 267 (3GPP TS 11.14)". To initiate a mobile transaction, the mobile transaction client application 125 queries the profile of the mobile device 110 to obtain information on support for BIP commands, available BIP channels and available BIP transport interfaces. FIG. 4A, FIG. 4B, and FIG. 4C depict the BIP proactive commands, supported bearers, and supported transport interfaces, respectively. The BIB proactive commands include OPEN CHANNEL, CLOSE CHANNEL, RECEIVE DATA, SEND DATA, and GET CHANNEL STATUS. The supported bearers include Circuit Switched Data (CSD) and GPRS. The supported transport interfaces include Transmission Control protocol (TCP), User Datagram Protocol (UDP), and Reserved for Future Use (RFU). The mobile transaction client application 125 opens the appropriate channel using the appropriate transport interface and transmits data to a mobile transaction server application 141 residing within the server 140. The initiation of a mobile transaction can be triggered by user selection on the mobile device 110, by an event occurring on a mobile transaction server application 141 or automatically by an event occurring on a mobile transaction client application 125. The server 140 also connects to other servers 150 via the second network 80 and the mobile transaction server application141 transmits data to the additional servers 150.

In one example, the first network 90 is a wireless telecommunication network such GSM, GPRS, 3G, EDGE, CDMA, TDMA, WCDMA, Mobitex, or DataTac. In other examples first network 90 is a wireless local area network (WLAN) (i.e., 802.11x), a wireless personal area network (WPAN), a wired telecommunications network, a local area network (LAN), a personal area network (PAN) (i.e., Bluetooth, Infrared), or a direct serial line connection to server 140. In one example, the second network 80 is the Internet. In other examples, the second network 80 is a wired or a wireless telecommunication network, a local area network (LAN), a wireless wide area network (WWAN), a wireless local area network (WLAN), or a personal area network (PAN).

Mobile Operator Gateway 130 is a routing server utilized by the mobile operator to connect the mobile operator's private network to the public Internet, thereby enabling the mobile device110 to access nodes, servers and /or resources on the Internet.

Referring to FIG. 3, in other embodiments, the remote server 140 is another type of remote or local device such as a printer 142, a personal computer 143 or another mobile phone 141. In these embodiments the mobile device 110 supports the appropriate channels 115 to establish a connection with these types of remote or local devices. Examples of appropriate communication channels 115 include Infrared, Bluetooth, direct serial line connection, WLAN, LAN, GPRS, and PAN. In one example, the mobile transaction system 100 utilizes the Infrared, Bluetooth or serial connection of the mobile device 110 to send data to a printer 142 to print out a sales receipt. In another example the mobile transaction system 100 utilizes the Infrared, Bluetooth or serial connections of the mobile device 110 to connect to a server 140 and/or 150. In another example the mobile transaction system 100 utilizes the Infrared, Bluetooth or serial connections of the mobile device 110 to connect to an additional mobile devices 141 for data exchange.

In one embodiment, the mobile transaction system 100 is used for processing mobile payments, such as credit card transactions through the mobile device 110. In this embodiment the server 140 is a payment transaction server and the other servers 150 are payment processors and/or a payment gateway. In another embodiment, the mobile transaction system 100 is utilized for downloading "digital goods" from servers 140, 150 to mobile device 110 and/or to mobile device attachment 120 and to payment cards or smart cards that can connect to the mobile device 110 or the mobile device attachment 120. Examples of "digital goods" include electronic cash (e-Cash), electronic tickets (e-Tickets), electronic coupons (e-Coupons), loyalty points (i.e. frequent flyer miles, frequent shopper points), credits for pre-paid mobile airtime, credits for pre-paid utilities, and digital rights management (DRM) certificates for accessing multi-media applications from servers 140,150 to mobile device 110 and/or to the mobile device attachment 120 and payment card and/or smart card (not shown) in connection with mobile device 110 and/or mobile device attachment 120. This application is described in a co-pending

patent application entitled "System And Method For Mobile Payment And Fulfillment Of Digital Goods", the entire content of which is incorporated herein by reference.

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is: